RECEIVED
CENTRAL FAX CENTER
AUG 07 2006

ZILKA·KOTAB
PC
ZILKA, KOTAB & FEECE™

100 PARK CENTER PLAZA, SUITE 300
SAN JOSE, CA 95113

TELEPHONE (408) 971-2573
FAX (408) 971-4660

FAX COVER SHEET

Date:	August 7, 2006	**Phone Number**	**Fax Number**
To:	Examiner Chea		(571) 273-8300
From:	Kevin J. Zilka		

Docket No.: NAI1P056_01.187.01 **App. No: 10/028,650**

Total Number of Pages Being Transmitted, Including Cover Sheet: 31

Message:

Please deliver to Examiner Chea.

Thank you,

Kevin J. Zilka

☐ *Original to follow Via Regular Mail* X *Original will Not be Sent* ☐ *Original will follow Via Overnight Courier*

IF YOU DO NOT RECEIVE ALL PAGES OR IF YOU ENCOUNTER
ANY OTHER DIFFICULTY, PLEASE PHONE April
AT (408) 971-2573 AT YOUR EARLIEST CONVENIENCE

PAGE 1/31 * RCVD AT 8/7/2006 7:17:12 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/10 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):06-48

RECEIVED
CENTRAL FAX CENTER

AUG 0 7 2006

Practitioner's Docket No. NAI1P056/01.187.01 ***PATENT***

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Anton C. Rothwell et al.

Application No.: 10/028,650 Group No.: 2153
Filed: 12/20/2001 Examiner: Chea, Philip J.
For: EMBEDDED ANTI-VIRUS SCANNER FOR A NETWORK ADAPTER

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION--37 C.F.R. § 41.37)

1. This brief is in furtherance of the Notice of Appeal filed 02/03/2006, a substitute for the Appeal Brief filed 04/03/2006, and in response to the Notification of Non-Compliant Appeal Brief mailed on 07/05/2006.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10*
(When using Express Mail, the Express Mail label number is mandatory;
Express Mail certification is optional.)

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

_ deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. § 1.8(a)
_ with sufficient postage as first class mail.

37 C.F.R. § 1.10*
_ as "Express Mail Post Office to Addressee"
Mailing Label No. _____ (mandatory)

TRANSMISSION

✓ facsimile transmitted to the Patent and Trademark Office, (571) 273 - 8300.

April Skovmand
Signature

Date: 8/7/2006

April Skovmand
(type or print name of person certifying)

** Only the date of filing (' 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under ' 1.8 continues to be taken into account in determining timeliness. See ' 1.703(f). Consider "Express Mail Post Office to Addressee" (' 1.10) or facsimile transmission (' 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.*

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. §1.17(c), the fee for filing the Appeal Brief has already been paid. However, the Commissioner is authorized to charge any fees that may be due to deposit account 50-1351 (NAI1P056).

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant(s) believe that no Extension of Time is required; however, if it is determined that such an extension is required, Applicant(s) hereby petition that such an extension be granted and authorize the Commissioner to charge the required fees for an Extension of Time under 37 CFR 1.136 to Deposit Account No. 50-1351.

5. TOTAL FEE DUE

Applicant believes that only the above fees are due in connection with the filing of this paper because the appeal brief fee was paid with a previous submission. However, the Commissioner is authorized to charge any additional fees that may be due (e.g. for any reason including, but not limited to fee changes, etc.) to deposit account 50-1351 (Order No. NAI1P056).

6. FEE PAYMENT

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P056).

A duplicate of this transmittal is attached.

Signature of Practitioner
Kevin J. Zilka
Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120
USA

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

RECEIVED
CENTRAL FAX CENTER

AUG 0 7 2006

COPY

Practitioner's Docket No. NAI1P056/01.187.01 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Anton C. Rothwell et al.

Application No.: 10/028,650 Group No.: 2153
Filed: 12/20/2001 Examiner: Chea, Philip J.
For: EMBEDDED ANTI-VIRUS SCANNER FOR A NETWORK ADAPTER

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION–37 C.F.R. § 41.37)

1. This brief is in furtherance of the Notice of Appeal filed 02/03/2006, a substitute for the Appeal Brief filed 04/03/2006, and in response to the Notification of Non-Compliant Appeal Brief mailed on 07/05/2006.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10*

(When using Express Mail, the Express Mail label number is mandatory; Express Mail certification is optional.)

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

_ deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. § 1.8(a)
_ with sufficient postage as first class mail.

37 C.F.R. § 1.10*
_ as "Express Mail Post Office to Addressee"
Mailing Label No. _____ (mandatory)

TRANSMISSION

✓ facsimile transmitted to the Patent and Trademark Office, (571) 273 - 8300.

Signature: April Skovmand

Date: 8/7/2006

April Skovmand
(type or print name of person certifying)

** Only the date of filing (' 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under ' 1.8 continues to be taken into account in determining timeliness. See ' 1.703(f). Consider "Express Mail Post Office to Addressee" (' 1.10) or facsimile transmission (' 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.*

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. §1.17(c), the fee for filing the Appeal Brief has already been paid. However, the Commissioner is authorized to charge any fees that may be due to deposit account 50-1351 (NAI1P056).

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant(s) believe that no Extension of Time is required; however, if it is determined that such an extension is required, Applicant(s) hereby petition that such an extension be granted and authorize the Commissioner to charge the required fees for an Extension of Time under 37 CFR 1.136 to Deposit Account No. 50-1351.

5. TOTAL FEE DUE

Applicant believes that only the above fees are due in connection with the filing of this paper because the appeal brief fee was paid with a previous submission. However, the Commissioner is authorized to charge any additional fees that may be due (e.g. for any reason including, but not limited to fee changes, etc.) to deposit account 50-1351 (Order No. NAI1P056).

6. FEE PAYMENT

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P056).

A duplicate of this transmittal is attached.

Signature of Practitioner
Kevin J. Zilka
Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120
USA

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

RECEIVED
CENTRAL FAX CENTER

AUG 0 7 2006

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	
Rothwell et al.	Group Art Unit: 2153
Application No. 10/028,650	Examiner: Chea, Philip J.
Filed: 12/20/2001	Date: 08/07/2006
For: EMBEDDED ANTI-VIRUS SCANNER FOR A NETWORK ADAPTER	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

SUBSTITUTE APPEAL BRIEF (37 C.F.R. § 41.37)

This brief is in furtherance of the Notice of Appeal filed 02/03/2006, a substitute for the Appeal Brief filed 04/03/2006, and in response to the Notification of Non-Compliant Appeal Brief mailed on 07/05/2006 (see attached). While appellant disagrees with the Examiner as to whether the alleged deficiencies exist in the original Appeal Brief, a Substitute Appeal Brief with appropriate edits is nevertheless submitted to expedite prosecution.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

I REAL PARTY IN INTEREST
II RELATED APPEALS AND INTERFERENCES
III STATUS OF CLAIMS

IV STATUS OF AMENDMENTS

V SUMMARY OF CLAIMED SUBJECT MATTER

VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

VII ARGUMENT

VIII CLAIMS APPENDIX

IX EVIDENCE APPENDIX

X RELATED PROCEEDING APPENDIX

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is McAfee, Inc.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c) (1)(ii))

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no other such appeals, interferences, or related judicial proceedings.

A Related Proceedings Appendix is appended hereto.

III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-31, 33 and 34

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration: None
2. Claims pending: 1-31, 33 and 34
3. Claims allowed: None
4. Claims rejected: 1-31, 33 and 34
5. Claims cancelled: 32

C. CLAIMS ON APPEAL

The claims on appeal are: 1-31, 33 and 34

See additional status information in the Appendix of Claims.

IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

As to the status of any amendment filed subsequent to final rejection, an amendment was filed after final on 10/13/2005, and such amendment was entered.

V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

With respect to a summary of Claims 1, 14, 27, 28, and 29, as shown in Figures 2 and 3, a network adapter is provided including a processor (e.g. see item 302 of Figure 3, etc) positioned on the network adapter coupled between a computer and a network (e.g. see item 235 of Figure 2, etc). In use, the processor (e.g. see item 302 of Figure 3, etc) is adapted for virus scanning and content scanning of network traffic transmitted between the computer and the network (e.g. see item 235 of Figure 2, etc). See, for example, page 8, line 4 – page 9, line 10 et al. In addition, the virus scanning (e.g. see item 310 of Figure 3, etc) utilizes virus signature files to scan for known types of malicious programs or data. See, for example, page 9, lines 4-15, et al. Also, the virus signature files are stored on non-volatile solid state memory on the network adapter (e.g. item 300 of Figure 3, etc). See, for example, page 9, lines 12-15 et al.

With respect to a summary of Claim 6, as shown in Figure 5, the manner in which the scanning is performed is capable of being user-configured (e.g. see item 514 of Figure 5, etc). See, for example, page 13, lines 16-22 et al.

With respect to a summary of Claim 11, as shown in Figures 3 and 4, the processor (e.g. see item 302 of Figure 3, etc) is capable of scanning (e.g. see item 418 of Figure 4, etc) received packets (e.g. see item 402 of Figure 4, etc) that are of interest (e.g. see item 406 of Figure 4, etc). See, for example, page 10, line 7 to page 12, line 2 et al.

With respect to a summary of Claim 30, as shown in Figure 3, the content scanning (e.g. see item 310 of Figure 3, etc) enforces operational policies of an organization. See, for example, page 9, lines 4-10 et al.

With respect to a summary of Claim 33, as shown in Figures 3 and 5, the memory is user protected by configuring a network adapter (e.g. see item 300 of Figure 3, etc) BIOS with a password that only a user can change. See, for example, page 9, lines 12-15 et al.

VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue # 1: The Examiner has rejected Claims 1-32 and 34 under 35 U.S.C. 103(a) as being unpatentable over Nessett et al. (U.S. Patent No. 5,968,176) in view of Reid et al. (U.S. Patent No. 6,182,226) in further view of Kephart (U.S. Patent No. 5,452,442).

Issue # 2: The Examiner has rejected Claim 33 under 35 U.S.C. 103(a) as being unpatentable over Nessett et al. (U.S. Patent No. 5,968,176) in view of Reid et al. (U.S. Patent No. 6,182,226) in view of Kephart (U.S. Patent No. 5,452,442) in further view of Bonomo et al. (U.S. Patent No. 6,658,562).

VII ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

Issue # 1:

The Examiner has rejected Claims 1-32 and 34 under 35 U.S.C. 103(a) as being unpatentable over Nessett et al. (U.S. Patent No. 5,968,176) in view of Reid et al. (U.S. Patent No. 6,182,226) in further view of Kephart (U.S. Patent No. 5,452,442).

Group #1: Claims 1-5, 7-10, 12-29, 31, 32 and 34

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

With respect to the first element of the prima facie case of obviousness and, in particular, the obviousness of combining the aforementioned references, the Examiner argues that a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Nessett by employing a firewall capable of virus scanning to scan for known types of malicious programs or data, as in Reid et al., in order to further improve the level of security provided by a firewall to prevent malicious attacks from incurring on a target system. The Examiner also argues that a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Nessett in view of Reid et al., by scanning for virus signature files, such as disclosed by Kephart, in order to accurately monitor for viruses, and distinguish false alarms from regularly executing programs. To the contrary, appellant

respectfully asserts that it would not have been obvious to combine the teachings of the Nessett, Reid and Kephart references, especially in view of the vast evidence to the contrary.

For example, Nessett relates to a **Network Interface Card (NIC)** firewall, while Reid relates to external firewalls. To simply glean features from a NIC firewall, such as that of Nessett, and combine the same with the *non-analogous art* of external firewalls, such as that of Reid would simply be improper. External firewalls protect multiple computers, while a NIC firewall protects the computer to which it is attached. "In order to rely on a reference as a basis for rejection of an appellant's invention, the reference must either be in the field of appellant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned." In re Oetiker, 977 F.2d 1443, 1446, 24 USPQ2d 1443, 1445 (Fed. Cir. 1992). See also In re Deminski, 796 F.2d 436, 230 USPQ 313 (Fed. Cir. 1986); In re Clay, 966 F.2d 656, 659, 23 USPQ2d 1058, 1060-61 (Fed. Cir. 1992) In view of the vastly different types of problems a NIC firewall addresses as opposed to an external firewall, the Examiner's proposed combination is inappropriate.

In addition, contrary to the Examiner's arguments, appellant's claimed feature would have been unobvious in view of Reid, since Reid' external firewalls *teach away* from any sort of processor positioned on a network adapter coupled between a computer and a network. *In re Hedges*, 783 F.2d 1038, 228 USPQ 685 (Fed. Cir. 1986).

Further, as noted above, Nessett relates to a firewall, while Kephart relates solely to virus scanning. To simply glean features from a firewall, such as that of Nessett, and combine the same with the *non-analogous art* of virus scanners, such as that of Kephart would simply be improper. Firewalls protect computers using rule-based filtering, while a virus scanner performs signature-based scanning. In view of the vastly different types of problems a firewall addresses as opposed to a virus scanner, the Examiner's proposed combination is again inappropriate.

In the Advisory Action dated 11/16/2005, the Examiner has responded to appellant's arguments by stating that "it is shown by Reid that firewalls are known to scan for viruses," that with respect to Kephart "it is old and well known to utilize virus signatures when scanning for viruses," that Nessett

"shows a firewall placed on a Network Interface Card," and, therefore, it would have been obvious to combine such references.

Appellant again asserts that Nessett relates to a **Network Interface Card (NIC) firewall**, while Reid relates to **external firewalls**. To simply glean features from a NIC firewall, such as that of Nessett, and combine the same with the *non-analogous art* of external firewalls, such as that of Reid would simply be improper. External firewalls protect multiple computers, while a NIC firewall protects the computer to which it is attached, thus making the respective environments and purposes of such arts un-combinable. In addition, contrary to the Examiner's arguments, appellant's claimed feature would have been unobvious in view of Reid, since Reid's external firewalls *teach away* from any sort of processor positioned on a network adapter coupled between a computer and a network. Still yet, Kephart only shows that it is well known to use virus signatures when scanning for viruses with a virus scanner, and not a firewall. Thus, it would not have been obvious to combine Kephart's teaching of virus signatures with the teaching of firewalls in Nessett and Reid.

More importantly, with respect to the third element of the prima facie case of obviousness, appellant respectfully asserts that the references relied on by the Examiner fail to meet appellant's claimed technique "wherein the virus signature files are stored on non-volatile solid state memory on the network adapter." Specifically, Examiner argues that "Nessett et al. in view of Reid et al. in view of Kephart further disclose that it would have been obvious to store the signature files on a non-volatile solid state memory on the network adapter since virus scanning is performed on the network adapter, it would be obvious that the signature files be located along with the virus scanner."

Appellant respectfully disagrees. Virus scanning on a network adapter, in and of itself, in no way makes it obvious that "the signature files be located along with the virus scanner," as purported by the Examiner. Just by way of example, the files may be alternatively stored on a host computer and retrieved as necessary to perform scanning.

Further, it appears that the Examiner has still not taken into consideration the full weight of appellant's claims. Specifically, the Examiner's proposed combination fails to even suggest a

technique "wherein the virus signature files are stored on non-volatile solid state memory on the network adapter." Such non-volatile feature provides numerous optional advantages such as scanning at boot-up (before signatures can be loaded into memory post-boot-up), etc.

In the Advisory Action dated 11/16/2005, the Examiner has argued that since "Nessett shows configuration data being stored on non-volatile memory in the device (read NIC)," it would have been obvious to "store the virus signature files along with the configuration data in the non-volatile memory in order to program the device and keep signature files updated with configuration data."

Appellant respectfully asserts that the configuration data in Nessett is only disclosed to include "filter parameters" (Col. 4, lines 25-26) and that "policy statements [are translated] into configuration data (Col. 4, line 36). Thus, the configuration data in no way relates to virus signatures but instead only relates to filter parameters and policy statements. Thus, it would not have been obvious to "store the virus signature files along with the configuration data in the non-volatile memory in order to program the device and keep signature files updated with configuration data," as the Examiner contends, since the configuration data in Nessett in no even relates to virus signature files.

Thus, with respect to at least the first and third elements of the prima facie case of obviousness, appellant respectfully asserts that the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #2: Claim 6

The Examiner has relied on Col. 7, lines 9-21 in Nessett to make a prior art showing of appellant's claimed technique "wherein the manner in which the scanning is performed is capable of being user-configured." Appellant respectfully asserts that such excerpt merely discloses filtering rules. Clearly, filtering rules do not meet appellant's specific claim language, namely "the manner in which the scanning is performed" (emphasis added), since filtering rules only identify types of data that may be allowed access, and not scanning, as claimed.

In the Advisory Action dated 11/16/2005, the Examiner has argued that "by setting filtering rules, you are telling the firewall to scan for different types of data and allow or deny access based on the scanning of the packet." The Examiner has also argued that the claim is unclear as to what manner the scanning is configured by the user.

First, appellant respectfully asserts that what is claimed is "the manner in which the scanning is performed" where the scanning is with respect to virus scanning and content scanning (see independent Claim 1 for context). Allowing a user to configure the manner in which the scanning itself is performed, as claimed by appellant, simply is not met by configuring the type of data to which filtering rules apply. Filtering rules only designate whether a packet is allowed or denied access, and configuring filtering rules therefore only allows for configuring which packets are allowed or denied access. To emphasize, the filtering rules simply have nothing to do with a manner in which the packets are scanned for viruses, but instead only relate to what the packets are scanned against.

In response to the Examiner's argument that the manner in which the scanning is configured is unclear and that the claim is thus unclear, appellant respectfully asserts that such claim language only claims that "the manner in which the scanning is performed is capable of being user-configured." Thus, the manner in which the configuration is performed is not the subject of the claim, but instead the subject is only that the manner in which the scanning is performed may itself be configured.

Thus, with respect to at least the third element of the prima facie case of obviousness, appellant respectfully asserts that the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #3: Claim 11

The Examiner has relied on Col. 23, lines 18-26 in Nessett to make a prior art showing of appellant's claimed technique "wherein the processor is capable of scanning received packets that are of interest." The Examiner further states that scanning is implied from the ability to distinguish between the different protocols. Appellant asserts that the Examiner has failed to

consider the full weight of appellant's claim language. Appellant claims "scanning received packets that are of interest," (emphasis added), and not simply firewalling received packets to determine if they are of interest, as in Nessett.

In the Advisory Action dated 11/16/2005, the Examiner has argued that "the system of combining Nessett in view of Reid in view of Kephart would allow one of ordinary skill in the art to see...a firewall embedded on a NIC, [and that] additionally containing a virus scanner would imply scanning packets that are of interest in order to quarantine the infected data and alert an administrator."

Appellant respectfully asserts that a virus scanner does not imply scanning packets that are of interest, but instead only generally implies scanning some sort of data. Nessett only relates to a firewall which itself determines the packets that are of interest (e.g. which packets are allowed), and not to "scanning received packets that are of interest," as claimed by appellant (emphasis added).

Thus, with respect to at least the third element of the prima facie case of obviousness, appellant respectfully asserts that the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #4: Claim 30

The Examiner has relied on Col. 17, lines 9-21 in Nessett to make a prior art showing of appellant's claimed technique "wherein the content scanning enforces operational policies of an organization." Appellant respectfully asserts that such excerpt only generally teaches managing security policy data. Clearly, managing security policy data for the operation of security systems, as in Nessett, does not meet any sort of content scanning, and especially not content scanning that "enforces operational policies in an organization," as specifically claimed by appellant.

In the Advisory Action dated 11/16/2005, the Examiner has argued that it is unclear what appellant means by content. The Examiner has taken the broadest interpretation of the claim and

has used content to mean the entire packet, including the header and payload. The Examiner has thus concluded that by changing filtering rules according to security policy management, Nessett shows that altering what is allowed or denied access through the firewall can change operational policies. Appellant respectfully asserts that what is claimed is that "the content scanning enforces operational policies of an organization," and not merely that "altering what is allowed or denied access through the firewall can change operational policies," as argued by the Examiner (emphasis added).

Thus, with respect to at least the third element of the prima facie case of obviousness, appellant respectfully asserts that the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Issue # 2:

The Examiner has rejected Claim 33 under 35 U.S.C. 103(a) as being unpatentable over Nessett et al. (U.S. Patent No. 5,968,176) in view of Reid et al. (U.S. Patent No. 6,182,226) in view of Kephart (U.S. Patent No. 5,452,442) in further view of Bonomo et al. (U.S. Patent No. 6,658,562).

Group #1: Claim 33

The Examiner has relied on Col. 4, lines 11-21 and 30-41 from Bonomo to make a prior art showing of appellant's claimed technique "wherein the memory is user protected by configuring a network adapter BIOS with a password that only a user can change." Appellant respectfully asserts that such excerpts only generally teach, with respect to a network adapter, that "an administrator password may boot from a floppy disk drive, a CD-ROM or ROM 104, or a network interface card 118" (see Col. 4, lines 28-30).

Merely booting from a network interface card (using a password) simply does not even suggest any sort of configuration of a network adapter BIOS with a password (that only a user can change), for the specific purpose of protecting the memory on the network adapter, as claimed by appellant.

Thus, with respect to at least the third element of the prima facie case of obviousness, appellant respectfully asserts that the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

VIII CLAIMS APPENDIX (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Presented) A network adapter system, comprising:
(a) a processor positioned on a network adapter coupled between a computer and a network;
(b) wherein the processor is adapted for virus scanning and content scanning of network traffic transmitted between the computer and the network;
(c) wherein the virus scanning utilizes virus signature files to scan for known types of malicious programs or data;
(d) wherein the virus signature files are stored on non-volatile solid state memory on the network adapter.

2. (Original) The network adapter system as recited in claim 1, wherein the processor is capable of being user-configured.

3. (Original) The network adapter system as recited in claim 2, wherein the processor is capable of being user-configured locally.

4. (Original) The network adapter system as recited in claim 2, wherein the processor is capable of being user-configured remotely via a network connection with the network adapter.

5. (Original) The network adapter system as recited in claim 2, wherein the processor is capable of being user-configured only after the verification of a password.

6. (Original) The network adapter system as recited in claim 2, wherein the manner in which the scanning is performed is capable of being user-configured.

7. (Original) The network adapter system as recited in claim 2, wherein the settings of the network adapter are capable of being user-configured.

8. (Original) The network adapter system as recited in claim 1, wherein the processor is capable of determining whether received packets are of interest.

9. (Original) The network adapter system as recited in claim 8, wherein the received packets are of interest based on an associated protocol.

10. (Original) The network adapter system as recited in claim 8, wherein the processor is capable of passing received packets that are not of interest to the computer.

11. (Original) The network adapter system as recited in claim 10, wherein the processor is capable of scanning received packets that are of interest.

12. (Original) The network adapter system as recited in claim 11, wherein the processor is capable of denying received packets that fail the scan.

13. (Original) The network adapter system as recited in claim 1, wherein the scan is performed based on user settings.

14. (Previously Presented) A method for scanning network traffic on a network adapter, comprising:

(a) receiving packets at a network adapter including a processor positioned thereon;

(b) virus scanning and content scanning of the packets utilizing the processor; and

(c) conditionally taking security measures if the packets fail the scan;

(d) wherein the virus scanning utilizes virus signature files to scan for known types of malicious programs or data;

(e) wherein the virus signature files are stored on non-volatile solid state memory on the network adapter.

15. (Original) The method as recited in claim 14, wherein the processor is capable of being user-configured.

16. (Original) The method as recited in claim 15, wherein the processor is capable of being user-configured locally.

17. (Original) The method as recited in claim 15, wherein the processor is capable of being user-configured remotely via a network connection with the network adapter.

18. (Original) The method as recited in claim 15, wherein the processor is capable of being user-configured only after the verification of a password.

19. (Original) The method as recited in claim 15, wherein the manner in which the scanning is performed is capable of being user-configured.

20. (Original) The method as recited in claim 15, wherein the settings of the network adapter are capable of being user-configured.

21. (Original) The method as recited in claim 14, wherein the processor is capable of determining whether received packets are of interest.

22. (Original) The method as recited in claim 21, wherein the received packets are of interest based on an associated protocol.

23. (Original) The method as recited in claim 22, wherein the processor is capable of passing received packets that are not of interest to the computer.

24. (Original) The method as recited in claim 23, wherein the processor is capable of scanning received packets that are of interest.

25. (Original) The method as recited in claim 24, wherein the processor is capable of denying received packets that fail the scan.

26. (Original) The method as recited in claim 14, wherein the scan is performed based on user settings.

27. (Previously Presented) A system for scanning network traffic on a network adapter, comprising:

(a) network adapter means for receiving packets;

(b) processor means positioned on the network adapter means for virus scanning and content scanning of the packets; and

(c) means for conditionally taking security measures if the packets fail the scan;

(d) wherein the virus scanning utilizes virus signature files to scan for known types of malicious programs or data;

(e) wherein the virus signature files are stored on non-volatile solid state memory on the network adapter means.

28. (Previously Presented) A system for scanning network traffic on a network adapter, comprising:

(a) network adapter means for receiving packets;

(b) logic positioned on the network adapter means for virus scanning and content scanning of the packets; and

(c) logic for conditionally taking security measures if the packets fail the scan;

(d) wherein the virus scanning utilizes virus signature files to scan for known types of malicious programs or data;

(e) wherein the virus signature files are stored on non-volatile solid state memory on the network adapter means.

29. (Previously Presented) A network adapter system, comprising:

(a) a processor positioned on a network adapter coupled between a computer and a network, the processor including a packet assembly module, random access memory (RAM), and a scanner module;

(b) a user interface driver for identifying network traffic of interest transmitted between the computer and the network;

(c) wherein the processor is adapted for discerning and virus scanning and content scanning of network traffic of interest transmitted between the computer and the network

(d) wherein the virus scanning utilizes virus signature files to scan for known types of malicious programs or data;

(e) wherein the virus signature files are stored on non-volatile solid state memory on the network adapter.

30. (Previously Presented) The network adapter system as recited in claim 1, wherein the content scanning enforces operational policies of an organization.

31. (Previously Presented) The network adapter system as recited in claim 30, wherein the policies include detecting entities selected from the group consisting of harassing content, pornographic content, junk e-mails, and misinformation.

32. (Cancelled)

33. (Previously Presented) The network adapter system as recited in claim 1, wherein the memory is user protected by configuring a network adapter BIOS with a password that only a user can change.

34. (Previously Presented) The network adapter system as recited in claim 11, wherein the received packets that are of interest include executable files.

IX EVIDENCE APPENDIX (37 C.F.R. § 41.37(c)(1)(ix))

There is no such evidence.

X RELATED PROCEEDING APPENDIX (37 C.F.R. § 41.37(c)(1)(x))

There is no such related proceeding.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P056/01.187.01).

Respectfully submitted,

By: _____ Date: 8/07/06

Kevin J. Zilka

Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/028,650	12/20/2001	Anton C. Rothwell	NAI1P056/01.187.01	2721

28875 7590 07/05/2006

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
ART UNIT	PAPER NUMBER

DATE MAILED: 07/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Notification of Non-Compliant Appeal Brief (37 CFR 41.37)	Application No. 10/028,650	Applicant(s) ROTHWELL ET AL.	
	Examiner Philip J. Chea	Art Unit 2153	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

The Appeal Brief filed on *03 April 2006* is defective for failure to comply with one or more provisions of 37 CFR 41.37.

To avoid dismissal of the appeal, applicant must file anamended brief or other appropriate correction (see MPEP 1205.03) within **ONE MONTH or THIRTY DAYS** from the mailing date of this Notification, whichever is longer. **EXTENSIONS OF THIS TIME PERIOD MAY BE GRANTED UNDER 37 CFR 1.136.**

1. ☒ The brief does not contain the items required under 37 CFR 41.37(c), or the items are not under the proper heading or in the proper order.

2. ☐ The brief does not contain a statement of the status of all claims, (e.g., rejected, allowed, withdrawn, objected to, canceled), or does not identify the appealed claims (37 CFR 41.37(c)(1)(iii)).

3. ☐ At least one amendment has been filed subsequent to the final rejection, and the brief does not contain a statement of the status of each such amendment (37 CFR 41.37(c)(1)(iv)).

4. ☒ (a) The brief does not contain a concise explanation of the subject matter defined in each of the independent claims involved in the appeal, referring to the specification by page and line number and to the drawings, if any, by reference characters; and/or (b) the brief fails to: (1) identify, for each independent claim involved in the appeal and for each dependent claim argued separately, every means plus function and step plus function under 35 U.S.C. 112, sixth paragraph, and/or (2) set forth the structure, material, or acts described in the specification as corresponding to each claimed function with reference to the specification by page and line number, and to the drawings, if any, by reference characters (37 CFR 41.37(c)(1)(v)).

5. ☐ The brief does not contain a concise statement of each ground of rejection presented for review (37 CFR 41.37(c)(1)(vi))

6. ☐ The brief does not present an argument under a separate heading for each ground of rejection on appeal (37 CFR 41.37(c)(1)(vii)).

7. ☐ The brief does not contain a correct copy of the appealed claims as an appendix thereto (37 CFR 41.37(c)(1)(viii)).

8. ☐ The brief does not contain copies of the evidence submitted under 37 CFR 1.130, 1.131, or 1.132 or of any other evidence entered by the examiner and relied upon by appellant in the appeal, along with a statement setting forth where in the record that evidence was entered by the examiner, as an appendix thereto (37 CFR 41.37(c)(1)(ix)).

9. ☐ The brief does not contain copies of the decisions rendered by a court or the Board in the proceeding identified in the Related Appeals and Interferences section of the brief as an appendix thereto (37 CFR 41.37(c)(1)(x)).

10. ☒ Other (including any explanation in support of the above items):

Heading VI is incorrectly identified as "Issues". The appropriate heading for section VI is "Grounds of rejection to be reviewed on appeal" At least page 1 and page 8 contain the incorrect heading.

Applicant has argued independent claims 1,14, and 27-29, in regards to the limitation "wherein the virus signature files are stored on non-volatile solid state memory on the network adapter", but have not referred to the specification by page and line number explaining the subject matter.

Applicant has argued dependent claims 6,11,30, and 33 separately, but have not set forth the structure, material, or acts described in the supporting specification. The Examiner kindly requests that each claimed function argued separetely be referenced to the specification by page and line number.

GLENTON B. BURGESS
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100